INFORMATION TRUST EXCHANGE GOVERNING ASSOCIATION

DRAFT DRAFT

EXCHANGE *GUIDE* / (RULES)

Ver. 2.1f / Jan. 11, 2017

Working draft / This document has status as a "Guide" for founding members and supporters of the ITEGA. A task group appointed by the ITEGA Board of Directors will be asked to prepare a document which can be adopted as "Rules" which will bind members' operations after Dec. 31, 2018. Please address comments on this draft guide to Bill Densmore (wpdensmore@gmail.com)

CONTENTS:

VERSION CONTROL PAGE

1.0 Preamble

This document defines the business and technical rules to be observed by entities which operate or own services licensed or sanctioned by the Information Trust Exchange Governing Association (hereinafter, "ITEGA") or which are members (statutory or non-statutory) of ITEGA; in particular those entities which have been assigned a global unique Member ID.

Whereas, consistent with the Mission and Core Values as stated in its Bylaws, and to grow audiences, increase revenues and deepen user relationships the ITEGA and its Members seek to:

1.1 Establish rules for a trustworthy, open, transparent and competitive digital marketplace for the sharing both valuable information content and privacy-respecting control of users' identity information.

1.2 Help users regain control of their privacy and identity and reduce by market forces a proliferation of accountable "tracking" of user behavior.

1.3 Help publishers to improve the relevance and value of advertising through deeper privacy-by-design knowledge about their users

1.4 Move toward an open platform where a "fast pass for purchase of news (and information)" is possible.

1.5 Agree upon technical architecture, certain business rules, protocols and interfaces that work to assure an open market for digital information.

1.6 Achieve objectives under the guidance of a non-governmental, non-stock, public-benefit entity.

Now therefore it is stated:

2.0 Definitions

An "Entity" is a person, member, individual, corporation, a limited-liability company, joint venture, estate, trust or unincorporated organization or any governmental or any agency or political subdivision therefore.

A "Member" is an entity which has executed a Member Agreement with the ITEGA. A "member" encompasses such member's affiliates and its and their controlling persons, directors, officers, employees, agents and advisors.

A “User” is a member of the general public who accesses or uses services provided by one or more ITEGA members.

A “Publishing Member” (PubMbr) is an entity, defined more specifically in the ITEGA Member Services Agreement which produces or markets original content.

An “Identity Service Provider Member” (IdSP) is an entity, define more specifically in the ITEGA Member Services Agreement, which helps manages privacy, accounts, data and identity of Users.

A “Technology Service Member” (ServiceMbr) is an operator of ITEGA-sanction services as defined more particularly in the ITEGA Member Services Agreement.

“Personal Identifying Information” (PII) --- Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an entity intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media. (source: U.S. Dept. of Labor). Also, information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name. Also any **information** that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered **PII**. (Also see, Wikipedia entry). As defined by the U.S. General Services Administration, PII is “"information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc." See also NIST Guide to Protecting the Confidentiality of Personally Identifyable Information (April 2010)

3.0 _ Mutual Intentions

The ITEGA expects that members or entities operating, owning or using ITEGA-sanctioned services intend and believe that:

2.1 OPEN IDENTITY -- The public interest is best served by establishing a structure for trusted, accountable facilitation of Internet identity and privacy which is transparent and open, and not ultimately controlled by nations, states or private-stakeholder

interests.

2.2 OPEN RELATIONSHIPS -- All constituencies within the ITEGA membership and operating environment should be free to maintain relationships and operate existing or future services independent or in competition with ITEGA-sanctioned services.

2.3 IDENTITY SERVICE -- In order to collect and manage Personal Identifying Information about a public user, a member or entity must take on the role and responsibility of an Identity Service Provider (IdSP).

2.4 ADVERTISING ANONYMITY -- An advertiser should be able to address relevant consumers with a relevant message, and should be able to reward the user service provider (IdSP or PubMbr) – and even the user directly – for the privilege of delivering the message – without being able to identify or target a specific, known individual. In general, users are reached as part of an audience segment, rather than an individual.

2.5 PORTABLE IDENTITY -- A consumer user might want to manage, control and perhaps "own" elements of their personal identity, and have one account, one ID and one bill with which to use content or access services from multiple, otherwise independent sources.

2.6 COMPETITIVE PRICING -- A content provider (PubMbr) should be able to establish and vary pricing for discrete information objects in real time based on the user's identity, relationships and use.

2.7 TIERED PRICING -- A service provider (IdSP) should be able to make money by purchasing content at lower wholesale prices and reselling it at higher retailer prices to its public users, managing the spread as a business exercise.

4.0 Design principles

Seven design principles are common to all ITEGA-sanctioned services:

4.1 PUBLISHER / USER INDEPENDENCE – ("Allow silos to continue")

- CONSIDERATIONS: The same way that a merchant's decision to accept Visa or MasterCard does not preclude accepting other forms of payment, including the merchant's own in-house credit card, the ITEGA should not in any way prevent a publisher from continuing to use any other technology or service of the publisher's choice.
- *REQUIREMENTS: The ITEGA service designs must not prohibit or prevent publishers or users from using their own information exchange or value exchange*

mechanisms outside the ITEGA. Nothing will restrict or inhibit a participating affiliate or publisher from continuing to operate within their own or other's user-management or value-exchange sharing services. A good analogy might be to a department or big-box store that accepts Visa or Mastercard from casual customers, but also continues to offer its own store revolving credit card to its own high-affinity customers.

4.2 USER DATA SHARING AND FREEMIUM PRICING

- CONSIDERATIONS: In today's Web environment, "free" services have become the *defacto* standard because users are paying for these services with their data. In this sense personal data has become a very real "currency" whose worth represents a significant portion of the $60B digital advertising market. However the current market for "adtech" and "trading" in this information has enormous issues with regard to privacy, transparency, and lack of user permission, participation, or control.
- *REQUIREMENTS: Neither the Exchange itself nor its agents will have access to unencrypted PII about Users. Users can choose among competitive service providers based on a level-playing field negotiation of their respective privacy-management offers. The ITEGA system designs must provide an opt-in mechanism for users to be able to share selected aspects of their user profile and/or usage statistics with either: a) ITEGA member publishers directly, or b) ITEGA member usage aggregators. This mechanism must also provide an explicit means of value exchange to reward users for sharing this information.*

4.3 USER-CENTRIC IDENTITY

- CONSIDERATIONS: The burden of online login and account management is currently unmanageable for all but the most dedicated of users. The alternative—social login services such as those provided by Facebook, Google, Twitter, and others—currently have too many privacy and intermediation problems to be a sustainable solution for the ITEGA membership.
- *REQUIREMENTS: ITEGA system designs must enable users to employ unique identifiers that that are universally recognized across the ITEGA ecosystem, but do not require centralized registry services. ITEGA architectures must enable the user to authenticate the user's choice of unique, standard-format identifier to ITEGA publisher sites. This authentication must be able to meet system-wide identity levels of assurance (LOA) that also meet the LOA requirements of a specific ITEGA publisher. The ITEGA identifier architecture must enable users to control the levels privacy afforded by these identifiers in ITEGA-sanctioned interactions.*

4.4 USER ANONYMITY / PROFILE SHARING

- CONSIDERATIONS: To gain marketer/advertiser participation, the Information Trust Exchange must support mechanisms for aggregating and sharing demographic,

interest and preference data about individual users upon transparent terms acceptable to the individual. This calculus inherently raises issues of personal privacy for end users. Also, in the same way the non-digital economy supports cash purchases in which a buyer does not reveal any information to a seller, ITEGA systems should enable purchases by users who choose not to reveal identity or profile information to a publisher. At the same time, ITEGA service providers who establish accounts and manage the "*persona*" and privacy of their users should be willing to share some demographic and interest information about their Users to third-party publishers as a condition of those publishers being willing to provide services to those users – in both cases to enhance the User experience.

- *REQUIREMENTS: The ITEGA sanctioned services should provide a standard mechanism for anonymous yet accountable purchases of content objects by ITEGA users. They should enable the serving of advertisements to individual users with specific interests within a cohort of other users – without advertisers or marketers having access to unique, personal identifying data about an individual user. ITEGA-sanctioned services will not enable the exchange of PII.*

4.5 USER CHOICE OF ACCOUNT HOSTING

- CONSIDERATIONS: Users will not adopt an ITEGA network that locks them into a single account host provider any more than they would adopt a banking network that locks them into a single bank. Having a choice from a competitive marketplace of ITE account host providers is as important as having a choice today from among a competitive marketplace of email account providers or cellular phone networks.
- *REQUIREMENTS: ITEGA-sanctioned systems must allow users to choose how their ITEGA-standard account will be hosted. Choices must include self-hosting and service provider hosting. For service provider hosting, the ITEGA design must provide options for both self-asserted assessment of compliance with ITEGA policies and reputation-based assessment. A user must be able to move (port) their ITEGA account and account data from one account host to another.*

4.6 PRICING CONTROLLED BY CONTENT OWNER

- CONSIDERATIONS: The value of news objects (stories, video, multimedia) vary widely based upon their timeliness, topic, type (long, short, investigative, narrative, spot, trade, MST) and application. News objects increasingly are disengaged from publisher packages by aggregation and "atomization." Therefore, royalty-owning publishers need a way to assign and transfer value (pricing) of individual objects across a sharing network. Royalty-pool models have largely failed because they remove the original publisher from value assignment.

- *REQUIREMENTS: ITEGA-compliant services must respect the pricing set by originating publishers (at wholesale), while allowing the free assignment of pricing at the consumer (retail) level. Designs must enable content objects to be sold on a bundled,*

subscription or a la carte basis. Content objects should be able to be made available on a bundled, subscription or a la carte basis, charge or free, as the owner wishes. It follows that publishers using ITEGA services must be willing to sell information resources to anonymized incoming casual or "drive-by" users (a la "newsstand customers") at a commercially reasonable price they establish, without having to know the identity or detailed information about these "guest" users.

4.7 USAGE BILLING AND SETTLEMENT

- CONSIDERATIONS: The overhead and friction of maintaining multiple payment options across multiple sites is currently prohibitive to all but the very largest publishers and payment service providers. Therefore it is paramount that the ITEGA facilitate the offering by and to members a network alternatives that reduces the costs and friction of all ITEGA payment options to an absolute minimum.
- *REQUIREMENTS: ITEGA designs must provide a standard mechanism for billing users for the content objects a user has consumed during an accounting period, and for settlement of a user account at the end of an accounting period. This billing and settlement mechanism must be as lightweight, low cost and low-friction as possible for both users and publishers.*

5.0 Core operating requirements

These operating requirements are proposed and sought as consistent with the strategic assumptions and design principles and should be part of ITEGA-sanctioned operations and specifications:

5.1 EVENT LOGGING -- Every HTTP action across the network that involves an exchange of value (a payment for an article or a reward for viewing or doing something) is logged to at least one neutral, third-party authentication and logging service, which is seen by the system participants as a "shared service" -- although in network practice it may be distributed and hierarchical as with Domain Name Service.

5.2 USER NETWORK OPACITY – An ITEGA-sanctioned logging service knows the user only by a unique alphanumeric identifier supplied by the user's "home base" registry service at the start of that particular session. Such logging services operate as agents, auditors and fiduciaries of publishers and user-registry services. As a matter of policy, ITEGA-sanctioned logging services shall not sell or provide clickstream data to ANYONE except to the user's home service provider (or their authorized agents) for their purposes (and for audit purposes to the publishing content provider if requested). The identifier -- to anyone other than the home base itself -- reveals nothing more than the identity of the user's home base.

5.3 SERVICE-PROVIDER CHOICE – There should evolve a plurality of home-base account

managers in the service (as there are thousands of home bases in Shiboleth/Internet2), providing end users a high degree of choice regarding business terms, especially as to identity and privacy.

5.4 VALUE AGGREGATION/SETTLEMENT -- At settlement time, the settlement service bundles event records -- sorted by home-base of the users on the one hand and by the vending publisher on the other hand -- and determines an aggregate debit or credit to charge the home base and an aggregated credit or debit to charge the publishers (note that a "publisher" could be a brand which is paying for a user to view a commercial message). This all is done periodically -- daily, weekly, monthly -- probably weekly in prototype – in reference implementation across the bank ACH or functionally equivalent network.

5.5 DISTRIBUTED DATA CONTROL -- The home base gets these bundled log reports and is free to sort them or use them as they wish (subject to their terms of service with the end user as to usage and privacy protection or not); in some cases there may be a discrete charge or payment to the end user for a particular access; in the vast majority of cases, one supposes, the home base will use the click-stream reports for demographic, marketing and business-model analysis but the end user will merely be paying a monthly subscription for some class of service.

5.6 AUDIT CAPABILITY -- The publisher (or information service provider), also gets bundled log reports of total usage so they can audit their payment or receipts, and the only sorting they are capable of doing is by the source of the end-user (i.e., their service-provider ID). Conceivably they might have methods to associate these anonymized usage reports to specific users, but the ITEGA may set business rules governing this practice and the rules would be enforceable by anything up to the ultimate sanction -- cutting a non-compliant information service provider off the system.

5.7 ENFORCEABILITY -- The provision for non-regulatory sanctions is one of the reasons why the governance and ownership of the service is so critical. The sanction of a network cutoff decision has to be the result of well-documented interchange rules (consider Visa as a model in this regard), and the entity making the decision has to have no competitive business interest one way or the other but rather only an interest in the fair administration of the service and due regard for evolving identity and privacy rights of end users. Hence, the need for a non-governmental and non-investor-owned entity with a mission to efficiently oversee and operate a service and not profit from it. Profit is for the publishers and service providers who use the service.

6.0 Operating technologies

Nine modules comprise the essential operations of an Information Trust Exchange Governing

Association ecosystem. Three are shared services; the rest are provided to ITEGA member publishers and service providers or by one or more technology vendors. They may be prototyped by one or multiple partners, vendors or members. The eight are listed below, with preliminary information about perceived options as of December, 2016.

A preliminary selection of best and alternative options for key operating technologies may be found at this lik:

https://www.dropbox.com/s/yoja7s1o9xe0zj7/ite-poc-testing-options-elements-v2-09-22-16.xls?dl=0

SHARED SERVICES RUN UNDER LICENSE TO THE ITEGA

6.1 Network user authentication services – This is a core feature of the ITEGA ecosystem – a method for "federated authentication" that allows an end User to be recognized and provided variable viewing, listening, access or payment rights and multiple independent web services. Over two decades, several well-understood, open-standard services have evolved for this purpose; ITEGA might select and enhance one with the ability to pass encrypted user data in standard formats.

6.2 Event/access logging service -- When an information resource is accessed by an end user – viewing an ad, reading an article, watching a video, listening to a podcast, an HTTP "event" is logged not only at the website providing the service, but also to a shared network service operated by one or more ITEGA-licensed vendors. This service is the second core component of the ITE shared-user network.

6.3 Aggregation and settlement services – The accumulated logging by the shared service of network events are sorted and aggregated by user service provider, by publisher or by data user (such as an advertiser or ad network) for settlement of debits/credits among the network members. Settlement is "notational" – it is not a banking or currency function. The results are both detailed and summary reports to publishers for royalty payments, and to service providers for purchase of content, for advertising charges and advertising revenue and to network participants who may be accruing transactional fees. Multiple examples of such aggregation and settlement services exist in banking, telecommunications, ad-tech, music and affiliate marketing and may be adapted to the ITEGA ecosystem.

ITEGA-CERTIFIED THIRD-PARTY SERVICES

6.4 Advertising exchange service – The just-announced TrustX service of the Digital Content Next trade association appears well positioned to disrupt the ad-technology stack with a non-profit service-bureau approach.

6.5 Profile-exchange service -- Enables access to and network sharing of user attributes for the purpose of determining types of services and their value to be provided to a user; and which is capable of varying services based upon such parameters as subscription-authorization levels and credit thresholds.

6.6 Billing services – Upon receiving notation of aggregation and settlement, publishers or service providers may direct bill or contract with agents to do billing. Multiple examples of such billing services exist in banking, retailing, travel and technology and one or more will be selected for the ITE ecosystem.

6.7 Publisher content access control – Offered by multiple vendors, or home-brewed by publishers, but dynamic pricing is rare and access options tend to be relatively inflexible. The challenge here is to build standards for cross-publisher interoperability and event reporting. Examples in news publishing include Clickshare, Piano Media and MediaSpan.

6.8 End-user content personalization services – With a few exceptions, such as Cxense and LifeStream/Taxonometrics, personalization tends to be a direct-to-consumer service from tech platforms rather than a white-label provision for publishers.

6.9 User identity data and privacy management – This is new, emerging category that can be provisioned by publishers who wish to manage data and privacy for their users, or by specialty providers of this service such as RespectNetwork. The ITEGA ecosystem requires that an end User have at least one designated "home base" that either manages profile and usage data for them or allows them to do it themselves. The network then exchanges user-permissioned data.

7.0 **OPERATING METHODS**

ITEGA believes its mission, values and intentions for its members and the public, may be realized by one or more of the following methods:

7.1 Collaboration around research and testing of key technologies

7.2 Creation and maintenance of a globally unique Member Identifier (MemberID), as described more fully in the Member Agreement.

7.3 Trustworthy transfer of user and transactional data across the public TCP/IP network (Internet) among and between (a) diverse point-of-service (POS) devices, such as laptops, smart phones and tablets and (b) ITEGA Members, including content providers (PubMbrs) and end-user service providers (IdSPs).

7.4 A set of transparent, shared rules and technology for sharing the handling of user identity, privacy and value exchange, whether payment for content or rewards for viewing commercial messages.

7.5 A defined governance structure, including membership rights and responsibilities

7.6 Establishment of privacy, trust and identity standards

7.7 Enforcement of rules regarding the sharing of user data and content and the licensing of their use

7.8 Facilitation of Internet-wide subscriptions and usage or viewing payments

7.9 Enabling of consumer choice for commerce and privacy

7.10 Enabling of a network-wide content subscription

7.11 Other Service Elements, Business Elements and trademark usage rules as defined in the Member Agreement.

8.0 CONTENT ACCESS, TAGGING AND SHARING

8.1 ACCESS – ITEGA shall publish and certify one or more methods and technologies for controlling access to digital data based upon the attributes of a user seeking access. A Member can continue to use other methods for access control with its own users or not-ITEGA users, but must use an ITEGA-certified method and technology if it wishes to offer access to users whose network UserID is affiliated with a different Member.

8.2 TAGGING – ITGA will endeavor to publish and sanction one or more methods for tagging content objections as to their subject-matter, value, viewing authorization and such other attributes as may facilitate commerce and rights management. A Member which wishes to derive value via the ITEGA for its content much adopt an ITEGA-sanctioned method, when published.

8.3 SHARING – ITEGA will sanction a “Standard Open User Protocol (SOUP)” (working title) as a standard method and technology for securely exchanging user demographic, interest, preferences, query threshholds and access-rights data among and between ITEGA Members and sanctioned services, including, but not necessarily limited to content servers, authentication servers, identity servers,

logging servers and user-management servers. ITEGA members must adopt a minimum-required implementation of SOUP.

9.0 USER PRIVACY, ANONYMITY AND DATA SHARING

9.1 PRIVACY EXPECTATION – Users who are uniquely identified by a Member through creation of an account, subscription, database entry, or the consolidation of event or activity log or other reports; or by any other means which permits their unique differentiation from other Users; or the collection of Personal Identifying Information; are entitled to an expectation of privacy.

9.2 ITEGA believes a transparent and competitive marketplace for provide information and user-identity services facilitates user privacy. Neither the ITEGA nor its Members shall maintain any central repository of personal identifying information (PII) across all services. An IdSP may maintain such records on its own Users subject to such ITEGA rules as may be promulgated regarding user-authorization, collection and use.

9.3 PRIVACY CHOICE ASSURANCE -- A Member shall not knowingly collect, or facilitate the collection by others, of PII or uniquely identifying information about a User without first obtaining and documenting, using a specific, independent process certified by ITEGA, the explicit approval of the User to do so. After Dec. 31, 2018, the means and documentation shall be in a form approved by the ITEGA, and evidence of noncompliance shall be grounds for suspension or termination of the MemberID of the Member until corrected.

9.4 USER IDENTITY MANAGEMENT – A Member providing registration and user-data-management services to Users (functioning as an Identity Services Provider, or IdSP) must participate in an ITEGA certification process, when available, which endeavors to ensure that Users can independently and easily enter, view, change and delete PII or other information unique to their relationship with the Member; as well as authorize or de-authorize the use of such information in specific and general contexts; and that the registration/enrollment process is clear and transparent as to data handling and privacy expectations. The Member should prominently disclosure to its Users its assertions about its right to keep and use information about a User after a User ends a business relationship the Member. Notice and choice regarding use of PII should be hallmarks of the relationship between the IdSP and its Users.

9.5 USER DATA SHARING – In order to facilitate commerce and support the creation of valuable information services Users may choose to permit the

collection and use of data about their actions, interest and preferences by specific choice. The offering of such a choice by an ITEGA PubMbr or IdSP shall include a statement of ways in which such information will be used by the Member, and the Member's considered assessment of the benefit the User receives as a result. Such a choice shall be documented for each User in a method capable of being audited by ITEGA. ITEGA members other than those operating as an IdSP shall not seek, acquire, maintain, compile, cross-reference or otherwise use any PII of ITGEA users. Oneward transfers of PII to a third party must be pursuant to these Exchange Rules. The transferring party must (1) transfer data only for "limited and specific purposes"; (2) ascertain that the agent is obligated to provide at least the same protections as required of the transferring party; (3) take reasonable steps to ensure processing consistent with these Rules (4) stop or reasonably remediate unauthorized process upon notice and (5) provide a summary or representative copy of relevant policies and agreements to the User or the ITEGA upon request and (6) provide a User opt-out function prior to disclosure of PII to third parties.[1]

9.6 USER DATA NORMALIZE – Members shall normalize their user data that is shared to a standard taxonomy of user attributes or "SOUP" (Standard Open User Profile) as issued from time to time by ITEGA.

9.7 ANONYMITY – To facilitate individual anonymity, Technology Service Members shall not collect, compile, aggregate or verify, by means of any ITEGA-sanctioned service, any data that is capable of being used to uniquely identify a person by name or specific device or by an assigned government- or privately-issued identification number or method. A ServiceMbr may collect and store access or event records of Users identified by a temporary, session-based identifier encrypted and issued by the User's IdSP. Such records may be retained only so long as to be used for purposes of billing or advertising "frequency capping" analysis.

9.8 RETENTION -- Neither ITEGA nor its Technical Service Members shall retain or use any data which uniquely identifies a User longer than necessary to prepare and verify billing for services.

10.0 **USER AUTHENTICATION, ACCESS AND LOGGING**

[1] -- This language in this sentence is substantially taken with appreciation from a *National Law Review* article of March 1, 2016, "Privacy Shield: Top Five Reasons It's Tougher Than Safe Harbor, Whether you Should Certify and Next Steps," by Kurt Wimmer, David Bender and Caleb Skeath. Access Jan. 11, 2017 from: http://www.natlawreview.com/article/privacy-shield-top-five-reasons-it-s-tougher-safe-harbor-whether-you-should-certify

ITEGA-sanctioned authentication, authorization and logging services operate to facilitate access to public-network information services in such a way that the User's right of access, confirmation of viewing, or method of payment, among other things, may be assured. Such Authentication and Logging Services, operated by Technology Service Members, shall not require, accept nor store any PII or any uniquely identifying information other than a temporary, session-based identifier, encrypted and issued by the User's IdSP.

(See "Functional specifications for user-data sharing" for more detailed prototype design.)

Accordingly:

10.1 An IdSP shall have means to encrypt a session-based identifier for one of its Users, and send that identifier, along with other service or preference information to an auth/logging service.

10.2 The auth/logging service shall have a means to establish a session token for the User so identified, and return session information to the IdSP.

10.3 The IdSP shall have a means to assist the User to provide the session token to other ITEGA Members so they may provide services to the User, which might include advertising and serving of other forms of digital information and services.

10.4 Either a PubMbr or ServiceMbr, or both, shall have means to transmit to an appropriate auth/logging service a record of service provided which may include the unique, encrypted session token of the particular anonymous User.

10.5 Auth/logging services shall have means to accept such records and store them temporarily for Settlement and Billing.

10.6 Such records of exchange-facilitated activity will be aggregated, reported to IdSPs, PubMbrs and ServiceMbrs as permitted by Exchange Rules and only as required for business purposes, including value exchange. As a design requirement, ITEGA shared services (see paragraphs 6.1, 6.2 and 6.3, above) will not have access to unencrypted personal information about users.

11.0 VALUE, PRICING AND COMPETITION

11.1 VALUE-EXCHANGE METHODS – ITEGA intends that sanctioned services will support at least three forms of value exchange: (1) subscription bundles of content from multiple wholesale sources (2) Per-click purchase of individual objects where buyer's credit is verified (3) Rewards to end users, directly or indirectly, for their attention to commercial messages.

11.2 COMPETITIVE PRICING -- Content originators operating as PubMbrs shall, if they wish, be able to set their selling price at wholesale in a free market for digital information for individual content objects. IdSPs, other PubMbrs and ServiceMbrs will be able to purchase rights to such content at the offered (or a negotiated) price and may then resell those rights to Users at whatever price and in whatever fashion they wish. Royalty-owning publishers shall have the right and capability to assign pricing directly to their own users and indirectly (wholesale) to other ITEGA members. Members shall not dictate pricing of content use at the retail level. Their choice is to sell or not to sell at wholesale across ITEGA. Content objects sold by a PubMbr at wholesale must be available for sale (at a price set by the retailing IdSP) on a bundled, subscription or *a la carte* basis.

11.3 ANTI-MONOPOLY BEHAVIOR -- In order to facilitate a transparent and open market for digital information, neither the ITEGA nor its Members shall exchange or share information about pricing or service terms, which pricing terms shall be offered on like terms to like Users and competitors. Evidence of noncompliance with this Rule shall be grounds for suspension or permanent termination of the MemberID or IDs of noncompliant Members.

12.0 **ACCOUNTING, SETTLEMENT AND BILLING**

12.1 ACCCOUNTING – Accounting for value-exchange across ITEGA-sanctioned services will be based upon data, logged to an Authentication and Logging Service ("ALS"), of user events/activities within an ITEGA-sanctioned network. The logging includes specific attributes necessary for off-line aggregation and distribution of payments/charges. (Design goal: This happens without PII, just a alphaneumeric user ID that is opaque to all parts of the system except the user's identity service provider – their "home base.")

12.2 AGGREGATION – An ITEGA-sanctioned ALS performs the function of aggregating event/activity records by User within each IdSP in order to provide each IdSP records of the activities of its Users.

12.3 SETTLEMENT – The ALS also may prepare an aggregated Debit or Credit to each affiliated IdSP for transmission to an ITEGA-affiliated Technical Service Provider which is able to access payment networks such as the bank ACH network. The ALS establishes and enforces ITEGA-consistent rules for handling chargebacks and other disputes and provides activity reports to affiliated IdSPs.

12.4 BILLING – The billing of Debits or Credits is performed by one or more merchant processing or bank processing vends operating in the world banking networks. They are affiliated with an IdSP and an ALS but need not be directly affiliated with the ITEGA.

13.0 **OTHER TECHNOLOGY RULES**

THIS SPACE INTENTIONALLY LEFT BLANK

APPENDIX A

TECHNICAL REFERENCES:

1. Description of profile and content-sharing network

The ITEGA working document, "Technical description of a privacy-by-design customer profile and content sharing network" is a high-level narrative describing both system operation and proof-of-concept implementation and a diagram. A current version may be accessed from the following URL:
https://docs.google.com/document/d/1cJ51LaL4aq0NZ77Jnkc4lXVqfihxvvi2VsEkzrHXZOs/pub

2. _Services features and design specifications (Nov. 2015)

Following five task-group meetings during 2015, key members in November developed the document: "Information Trust Exchange Framework: Service Features and Design Specifications." The advisory document assembled a series of service goals – and resulting design requirements broad enough in scope to encompass further refinement around specific technologies or services not envisioned at that time. The completed document may be access from the following URL:
http://newshare.com/ite-next/ite-service-design-specs-v3-11-05-15.pdf

3. Functional specifications for user data sharing

The ITEGA working document, "Functional Specifications for User Data Sharing," proposes functional specifications for exchange of permissioned user data to support customized service of digital content – advertisements, stories or other services. A current version may be accessed from the following URL:
https://docs.google.com/document/d/1_n6swNv2bE7llM8F1uGaanyNOuAJohB88dwABF0Ab4w/pub

4. Working proposal for user profile attributes

The ITEGA working document, "User Profile Attributes" proposes an initial limited set of fields for exchanging use attributes across the ITE ecosystem. These consist of (1) Required user-supplied attributes (2) system-assigned network attributes (3) optional user-supplied demographic attributes (4) User expressed interest identities (5) Service preference-level attributes and (6) Active-inactive buyer tags. A current version of these profile attributes may be accessed from the following URL:
https://docs.google.com/spreadsheets/d/1i-7tEBGwqa7IUyFoworLEl4xIg1QeK_ryfVELS7NCbE/pubhtml

5. Proof-of-concept prototype elements

The ITEGA working document, "Proof-of-concept prototype elements provide a proposed phasing of elements of the ITE shared-user ecosystem. A current version may be accessed from the following URL:
https://docs.google.com/document/d/1UIuWk7c_opQHh15L8G9NhHCR7ADnyNN4NWUPZARmGiM/pub

The grid "Proof-of-concept test elements ranked, provides a list of 30 proof-of-concept test elements and ranks their priority for development. A version as of Sept. 25, 2016 may be found at this link:
https://docs.google.com/spreadsheets/d/1QJhrQZHduO5vGzXEg1ZPYS1mxxaK9XikZPCaVR_BGCk/pubhtml

APPENDIX B

Expected operating features

Here are nine expected operating features of ITEGA-compliant services which should be enabled and supported by the operating requirements:

- NETWORK SUBSCRIPTIONS – The service should allow publishers to be paid for providing digital content across an ITE network without having to have one-off relationship with each reader/user.

- DYNAMIC SERVICING – Publishers offering their content should have real-time personal, demographic, preference or interest attributes of a user/reader at the time the user makes an online/mobile request for information, so they can respond with targeted, customized messages or services.

- MICROACCOUNTING -- Publishers should not be required to participate in operations which "pool" royalties. Rather, a feature of the service should be census-type (vs. polling, pooling or sampling) logging and aggregation of billable content requests, with clearing-house settlement of payments and credits among publishers and user-account managers.

- WHOLESALE-RETAIL PRICING – Publishers shall be able to use one or more methods to establish the price they wish to receive (and be assured of payment) for a discrete digital object (or bundle), and be able to vary that price dynamically in real time based upon the attributes of the user requesting the object.

- ONE BILL/ACCOUNT –The service will enable a user/reader to have one bill/one account/single sign-on access to information from (virtually) anywhere, by subscription or by click/action?

- UNIVERSAL TRACKING – In order to gain the participation of publishers and advertisers, the system will enable a user's activity to be tracked across the ITE network and that activity aggregated – only -- to the user's home-base service provider for billing and analysis – contingent upon explicit permission of the user.

- CONTENT PACKAGING – In order to gain the participation of end users, publisher and billing-service users of the system should be able to facilitate custom assembly by the end user of information services from a variety of topical and geographic-oriented sources into personalized subscription packages.

- FREEMIUM vs. FREE – In order to gain participant of both privacy advocates and the advertising industry, the system should allow the public user to chose among a range of options from (1) no advertising and no disclosure or use of their tracked activity in a subscription-based approach to (2) receipt of highly customized commercial messages and the wide, background marketing of their information preferences in a rewards-based program approach.

- SUBSCRIPTION OR PER-CLICK – In order to satisfy the requirements of a plurality of publishers and service providers, the service should offer end users both sale or receipt of digital items within a pre-paid subscription package -- as well as being able to dynamically query the user if they want to purchase a particular resource on a one-time, one-item basis.

APPENDIX C

Project FAQ

1. **What are we trying to accomplish?** Make a marketplace for digital content -- convenient for the public, that allows personalization and respects privacy. A platform for content collaboration.

2. **Who are the customers?** B-to-B: Primary: News and digital content originators; Secondary: Advertisers, telcos, cable companies, retailers, associations. Goal: Help them deliver an incredible user experience through greater personalization and trusted privacy and identity management.

3. **Who are our partners?** Technology and publishing companies who will join the ITEGA and provide ITEGA-complaint services.

4. **What do we do for our partners?** Foster creation of a platform that enables a marketplace for them to make money through advertising, digital content sales and transaction fees.

5. **What is the role for RJI?** Provides ideas, fosters experiments, facilitates collaboration -- all with academic, foundation, media and technical partners -- which lead to the ITEGA formation and intended operation.

6. **What is the solution?** Based on 2011 and 2015 research reports, and O'Hare gathering proposed solution is a non-profit consortium which develops business rules and technical/design specifications for a "shared-user network for trust, identity, privacy and information commerce." Elements include:

    a. One-ID, one-bill account
    b. Choice of service providers
    c. Control of use of personal information
    d. Personalization options for content and ads enabled by vendors
    e. *A la carte* and bundled content purchasing; competition in pricing.

7. **What will sustain the ITEGA governing organization?** Initially grants, them

membership dues, then license fees from operators of network services (authentication, logging services).

VERSION CONTROL:

Ver. 2.1e / DEC. 28, 2016 – First complete writethrough by Bill Densmore Associates
Ver. 2.1f / Jan. 11, 2017 – Added privacy ideas from Kurt Wimmer's Privacy Shield 03-01-16 Privacy Shield post